Posudek oponenta bakalářské práce

Student: Vojanec Kamil
Téma: Ochrana před DoS útoky s využitím jazyka P4 (id 23113)
Oponent: Fukač Tomáš, Ing., UPSY FIT VUT

1. Náročnost zadání

obtížnější zadání

Zadání si vyžaduje seznámení se s relativně novým a zatím ne příliš rozšířeným jazykem P4. Dále bylo nutné se důkladně seznámit s aplikací DDoS Protector vyvíjenou sdružením CESNET, která je doposud ve fázi vývoje a dokumentace aplikace nejsou veřejně dostupné.

2. Splnění požadavků zadání

zadání splněno s drobnými výhradami

Body zadání byly splněny, avšak cílem bodu 3 a 4 měl být návrh a implementace rozšíření překladače o podporu funkcionalit potřebných pro realizaci zařízení zabraňujícímu DoS útokům. Některé však nebyly v rámci práce implementovány a nejsou stále podporovány, jak je uvedeno i v závěru práce. Úpravy software v návrhu nebyly uvažovány vůbec.

3. Rozsah technické zprávy

splňuje pouze minimální požadavky

Rozsah textu práce je přibližně 41 normostran a je doprovázen často nepřiměřeně velkými obrázky a příklady zdrojových kódů, které opticky navyšují rozsah práce.

4. Prezentační úroveň předložené práce

50 b. (E)

Jednotlivé kapitoly práce na sebe logicky navazují, jednotlivé informace v textu často nikoliv. Text díky tomu působí jako výčet nesouvisejících informací (např. kapitola popisující DDoS Protector). Kapitola popisující aplikaci DDoS Protector není příliš obsáhlá a nepopisuje aplikaci dostatečně. Popis způsobu testování byl jen krátce shrnut v kapitole 8. V textu nejsou sjednoceny názvy a střídají se anglické názvy s jejich doslovnými překlady (např. "DDoS" vs. "odepření přístupu", "DDoS Protector" vs. "čistička"), jsou používány zkratky, které nejsou zavedeny, popřípadě jsou zavedeny až později v textu (UH hlavička, SDM). Text je navíc nadměrně doplňován o odkazy na jiné části práce. Popisovaný kód je často uveden o několik stran dále v textu (např. text na stránce 19 popisuje kód na stránce 22). Text se proto velmi špatně čte, některé části nedávají dokonce smysl (např. odstavec "Útoky na úrovni operačního systému" na straně 11, popisy testů na straně 36). Text navíc často předpokládá, že má čtenář povědomí o činnostech probíhajících ve sdružení CESNET. Běžný čtenář si není schopen doplnit chybějící informace a práce může být pro něj nepochopitelná.

5. Formální úprava technické zprávy

75 b. (C)

Po jazykové stránce text obsahuje menší množství překlepů a nevhodně použitých slov a slovních obratů. Z hlediska typografie se v práci občas vyskytují jednoslabičné předložky na konci řádku, na stránku 30 je samostatně umístěn jen krátký odstavec textu na následující stránce je následně pouze jeden obrázek.

6. Práce s literaturou

50 b. (E)

Prameny použité pro popis jazyku P4 a DDoS útoků jsou voleny vhodně, nicméně některé části textu nejsou citovány (např. celé kapitoly 2.1, 2.2). V kapitole 4 je uveden jen jeden zdroj, popisující návrh zařízení pro ochranu před DoS útoky, ostatní informace v této kapitole však nejsou citovány vůbec. V celé práci se nenachází jediná citace obrázků, nejsou citována významná tvrzení, která jsou až zavádějící (např. "VHDL je jeden z nejpoužívanějších jazyků", "standardní rozhraní MI32").

7. Realizační výstup

75 b. (C)

V rámci práce byla do překladače P4-VHDL implementována podpora pro Match-Action tabulku využívající externí paměť, což umožňuje realizaci tabulky pro velké množstvím pravidel. Následně bylo pomocí jazyka P4 popsáno zařízení pro ochranu před DoS útoky a rozšířeným překladačem realizováno. U finálního řešení byla testována propustnost, která pro velké pakety dosahovala až ke 100 Gb/s. Překladač P4-VHDL bohužel nebyl rozšířen o některé funkcionality, které jsou důležité pro sběr statistických dat a mohou být pro některé navrhované aplikace klíčové.

8. Využitelnost výsledků

Práce popisuje realizaci již dříve navrženého zařízení pro ochranu před DoS útoky s využitím jazyka P4 a překladače P4-VHDL. Největší přínosem práce je integrace Match-Action tabulky využívající externí paměť do překladače P4-VHDL. Toto rozšíření umožňuje realizaci tabulek s velkou kapacitou v nejrůznějších P4 aplikacích. Realizované zařízení bude používáno a dále rozvíjeno ve sdružení CESNET.

9. Otázky k obhajobě

- V popisu architektury zařízení pro ochranu před DoS útoky byl uvedený prefixový filtr (obr. 4.3), proč však byl nahrazen filtrem realizující tzv. whitelist?

- Bylo by možné v Match-Action tabulce využívající externí paměť realizovat vyhledávací metodu longest prefix match (prefixový filtr)? Jaké úpravy by bylo nutné provést?

10. Souhrnné hodnocení

65 b. uspokojivě (D)

Vzhledem k značným výhradám k technické zprávě uděluji celkové hodnocení **D - uspokojivě**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 24. června 2020

Fukač Tomáš, Ing.
oponent